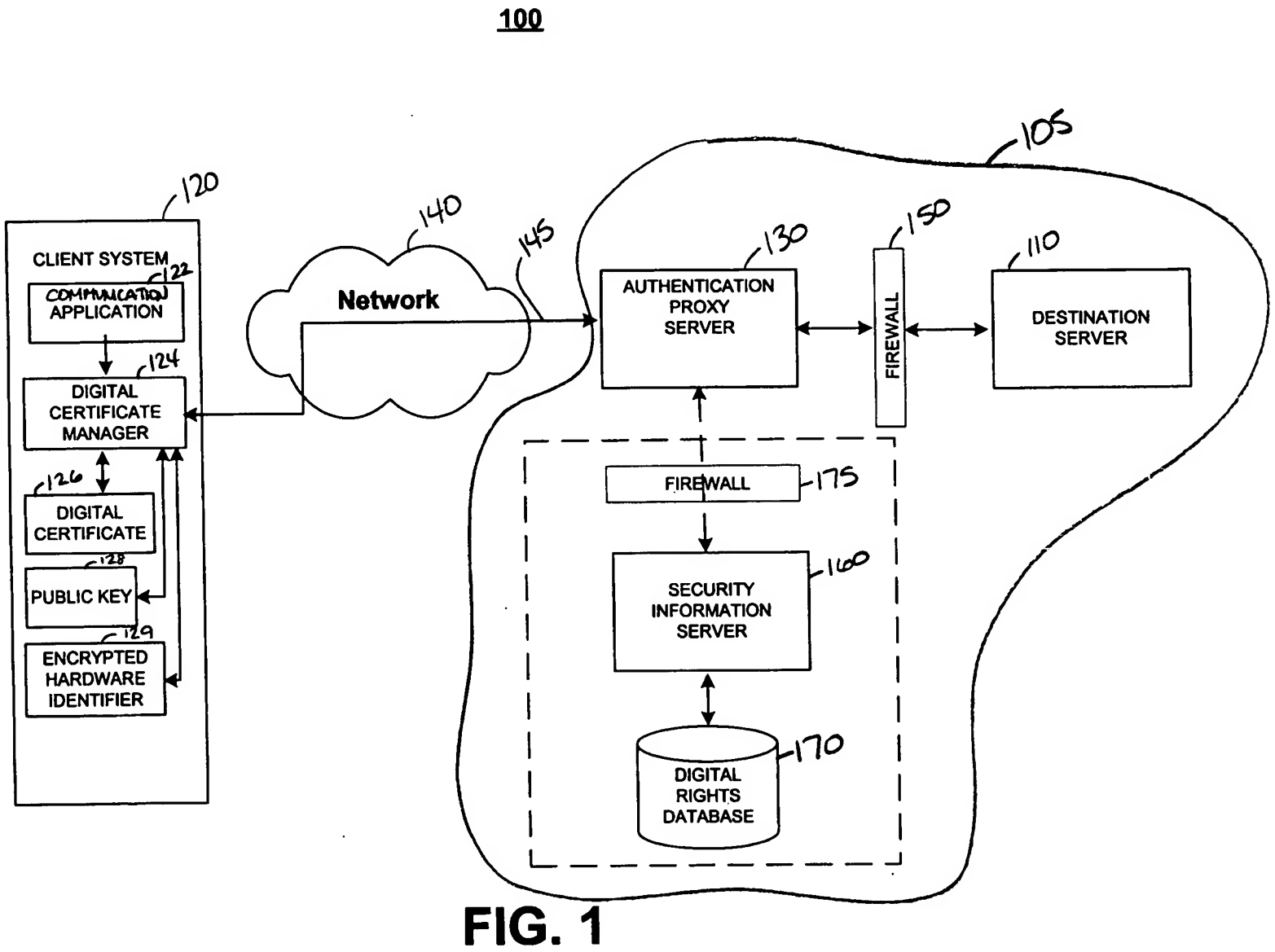
100
105
120
CLIENT SYSTEM
122
COMMUNICATION APPLICATION
124
DIGITAL CERTIFICATE MANAGER
126
DIGITAL CERTIFICATE
128
PUBLIC KEY
129
ENCRYPTED HARDWARE IDENTIFIER
140
Network
145
130
AUTHENTICATION PROXY SERVER
150
FIREWALL
110
DESTINATION SERVER
175
FIREWALL
160
SECURITY INFORMATION SERVER
170
DIGITAL RIGHTS DATABASE

FIG. 1

126

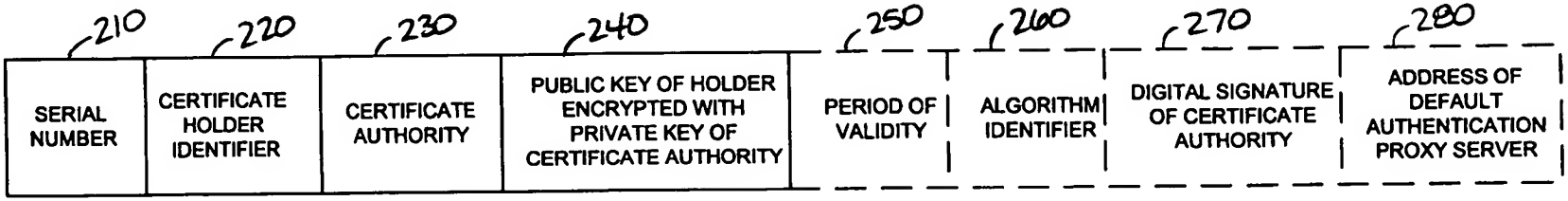
210
220
230
240
250
260
270
280
SERIAL NUMBER
CERTIFICATE HOLDER IDENTIFIER
CERTIFICATE AUTHORITY
PUBLIC KEY OF HOLDER ENCRYPTED WITH PRIVATE KEY OF CERTIFICATE AUTHORITY
PERIOD OF VALIDITY
ALGORITHM IDENTIFIER
DIGITAL SIGNATURE OF CERTIFICATE AUTHORITY
ADDRESS OF DEFAULT AUTHENTICATION PROXY SERVER

FIG. 2

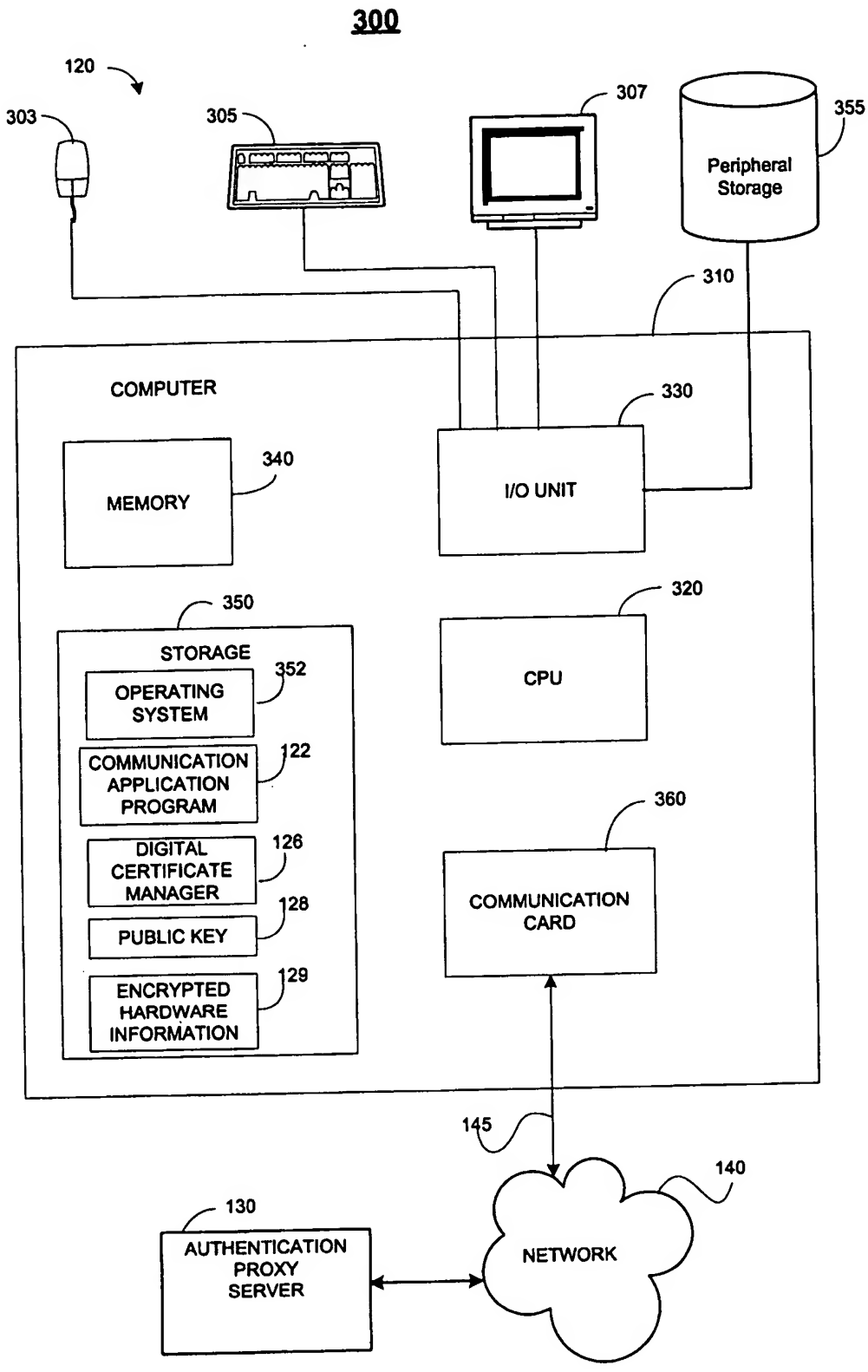
300
120
303
305
307
355
Peripheral Storage
310
COMPUTER
330
MEMORY
340
I/O UNIT
350
320
STORAGE
352
OPERATING SYSTEM
122
COMMUNICATION APPLICATION PROGRAM
126
DIGITAL CERTIFICATE MANAGER
128
PUBLIC KEY
129
ENCRYPTED HARDWARE INFORMATION
CPU
360
COMMUNICATION CARD
145
140
NETWORK
130
AUTHENTICATION PROXY SERVER

FIG. 3

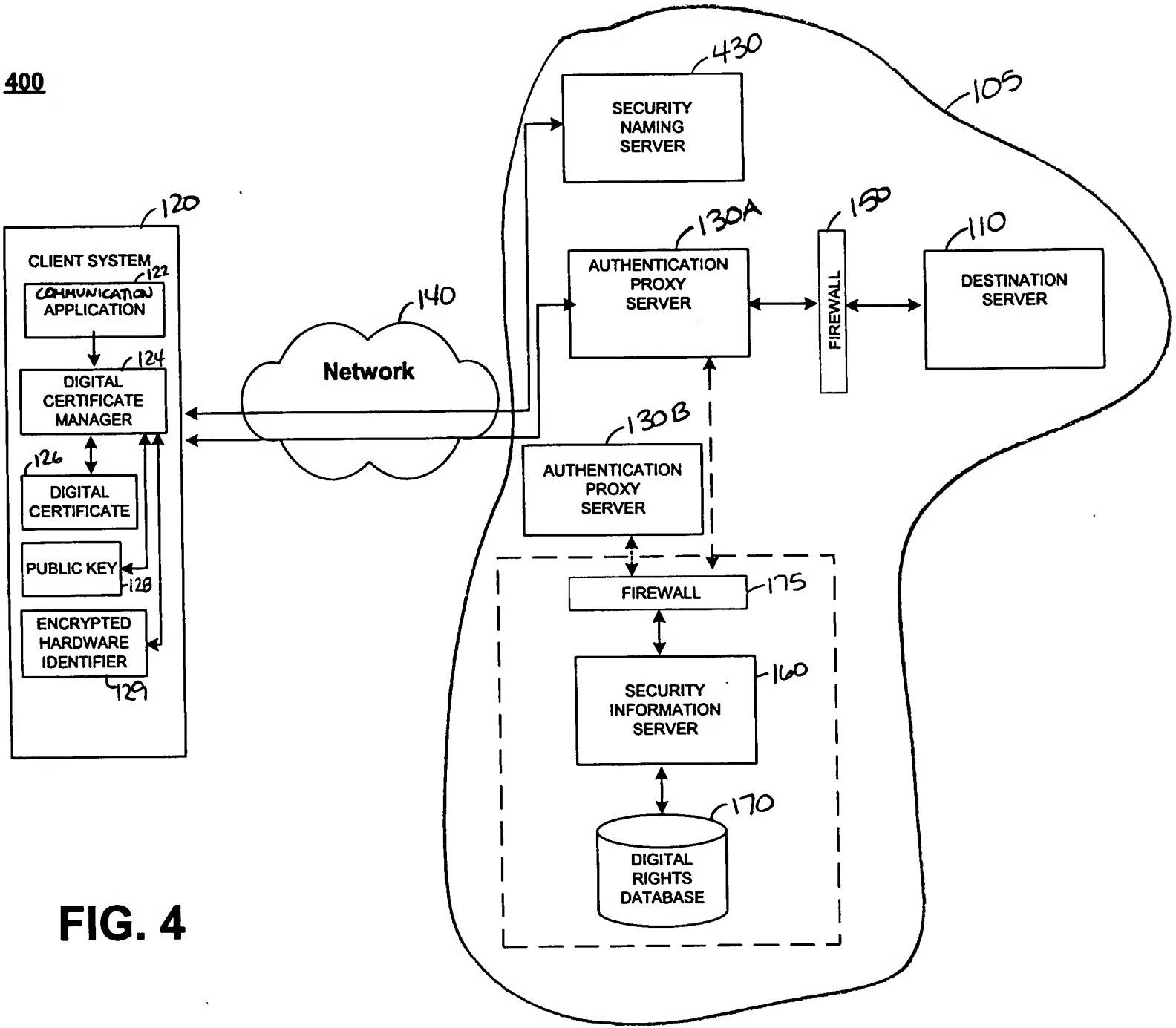
400
SECURITY NAMING SERVER
430
105
120
CLIENT SYSTEM
122
COMMUNICATION APPLICATION
140
Network
AUTHENTICATION PROXY SERVER
130A
150
FIREWALL
110
DESTINATION SERVER
124
DIGITAL CERTIFICATE MANAGER
130B
AUTHENTICATION PROXY SERVER
126
DIGITAL CERTIFICATE
PUBLIC KEY
128
FIREWALL
175
ENCRYPTED HARDWARE IDENTIFIER
129
SECURITY INFORMATION SERVER
160
170
DIGITAL RIGHTS DATABASE

FIG. 4

500

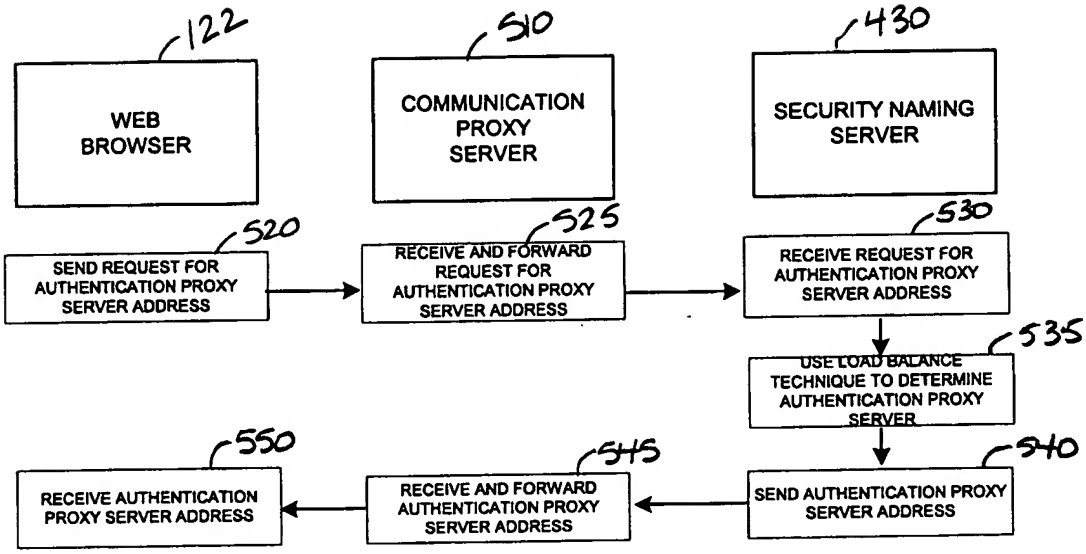
122
WEB BROWSER
510
COMMUNICATION PROXY SERVER
430
SECURITY NAMING SERVER
520
SEND REQUEST FOR AUTHENTICATION PROXY SERVER ADDRESS
525
RECEIVE AND FORWARD REQUEST FOR AUTHENTICATION PROXY SERVER ADDRESS
530
RECEIVE REQUEST FOR AUTHENTICATION PROXY SERVER ADDRESS
535
USE LOAD BALANCE TECHNIQUE TO DETERMINE AUTHENTICATION PROXY SERVER
540
SEND AUTHENTICATION PROXY SERVER ADDRESS
545
RECEIVE AND FORWARD AUTHENTICATION PROXY SERVER ADDRESS
550
RECEIVE AUTHENTICATION PROXY SERVER ADDRESS

FIG. 5

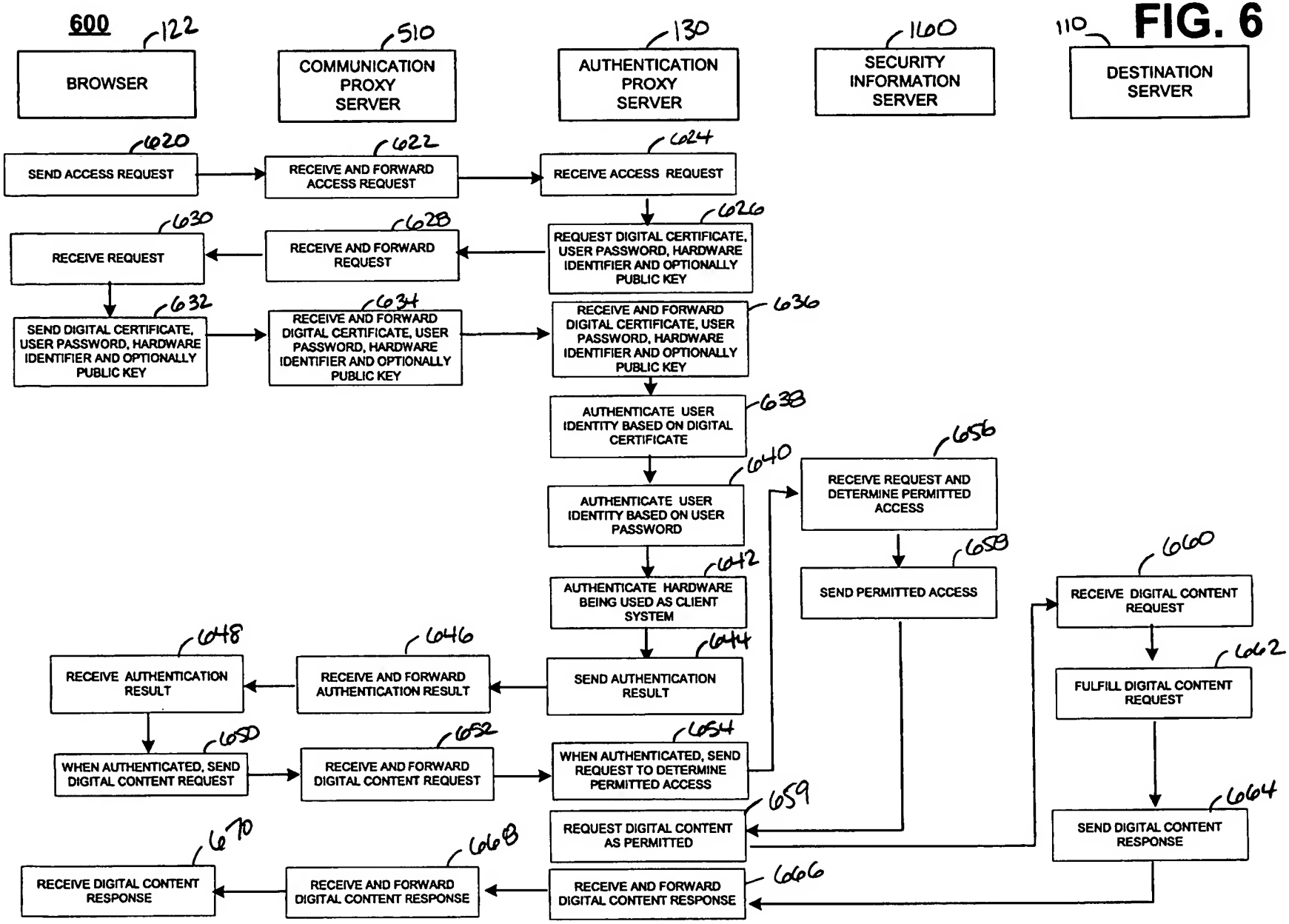
600
122
BROWSER
510
COMMUNICATION PROXY SERVER
130
AUTHENTICATION PROXY SERVER
1160
SECURITY INFORMATION SERVER
110
DESTINATION SERVER
6020
SEND ACCESS REQUEST
6022
RECEIVE AND FORWARD ACCESS REQUEST
6024
RECEIVE ACCESS REQUEST
6026
REQUEST DIGITAL CERTIFICATE, USER PASSWORD, HARDWARE IDENTIFIER AND OPTIONALLY PUBLIC KEY
6028
RECEIVE AND FORWARD REQUEST
6030
RECEIVE REQUEST
6032
SEND DIGITAL CERTIFICATE, USER PASSWORD, HARDWARE IDENTIFIER AND OPTIONALLY PUBLIC KEY
6034
RECEIVE AND FORWARD DIGITAL CERTIFICATE, USER PASSWORD, HARDWARE IDENTIFIER AND OPTIONALLY PUBLIC KEY
6036
RECEIVE AND FORWARD DIGITAL CERTIFICATE, USER PASSWORD, HARDWARE IDENTIFIER AND OPTIONALLY PUBLIC KEY
6038
AUTHENTICATE USER IDENTITY BASED ON DIGITAL CERTIFICATE
6040
AUTHENTICATE USER IDENTITY BASED ON USER PASSWORD
6042
AUTHENTICATE HARDWARE BEING USED AS CLIENT SYSTEM
6044
SEND AUTHENTICATION RESULT
6046
RECEIVE AND FORWARD AUTHENTICATION RESULT
6048
RECEIVE AUTHENTICATION RESULT
6050
WHEN AUTHENTICATED, SEND DIGITAL CONTENT REQUEST
6052
RECEIVE AND FORWARD DIGITAL CONTENT REQUEST
6054
WHEN AUTHENTICATED, SEND REQUEST TO DETERMINE PERMITTED ACCESS
6056
RECEIVE REQUEST AND DETERMINE PERMITTED ACCESS
6058
SEND PERMITTED ACCESS
6059
REQUEST DIGITAL CONTENT AS PERMITTED
6060
RECEIVE DIGITAL CONTENT REQUEST
6062
FULFILL DIGITAL CONTENT REQUEST
6064
SEND DIGITAL CONTENT RESPONSE
6066
RECEIVE AND FORWARD DIGITAL CONTENT RESPONSE
6068
RECEIVE AND FORWARD DIGITAL CONTENT RESPONSE
6070
RECEIVE DIGITAL CONTENT RESPONSE

FIG. 6

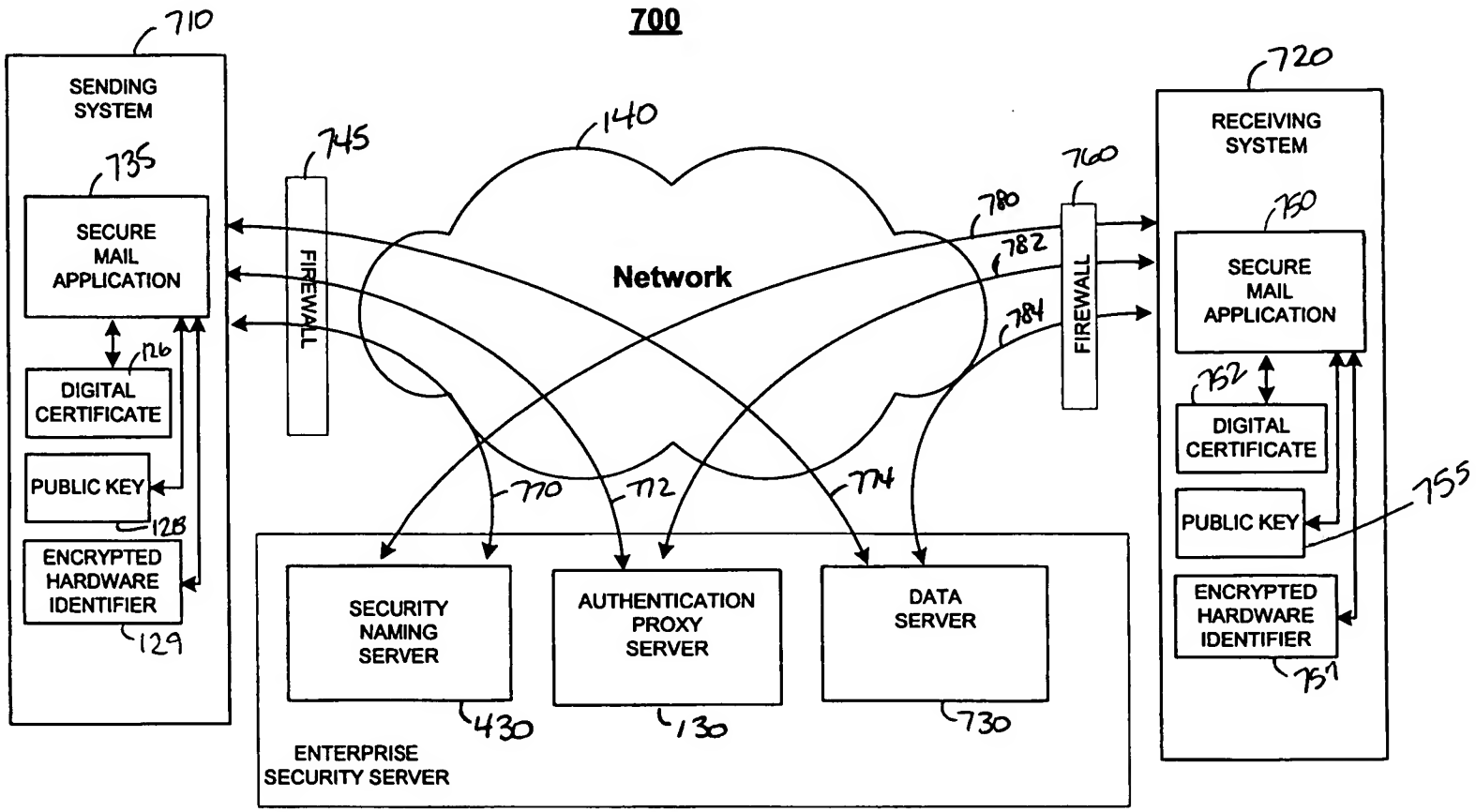
700
710
SENDING SYSTEM
735
SECURE MAIL APPLICATION
126
DIGITAL CERTIFICATE
PUBLIC KEY
128
ENCRYPTED HARDWARE IDENTIFIER
129
745
FIREWALL
140
Network
760
FIREWALL
780
782
784
720
RECEIVING SYSTEM
750
SECURE MAIL APPLICATION
752
DIGITAL CERTIFICATE
PUBLIC KEY
755
ENCRYPTED HARDWARE IDENTIFIER
751
770
772
774
SECURITY NAMING SERVER
430
AUTHENTICATION PROXY SERVER
130
DATA SERVER
730
ENTERPRISE SECURITY SERVER

FIG. 7

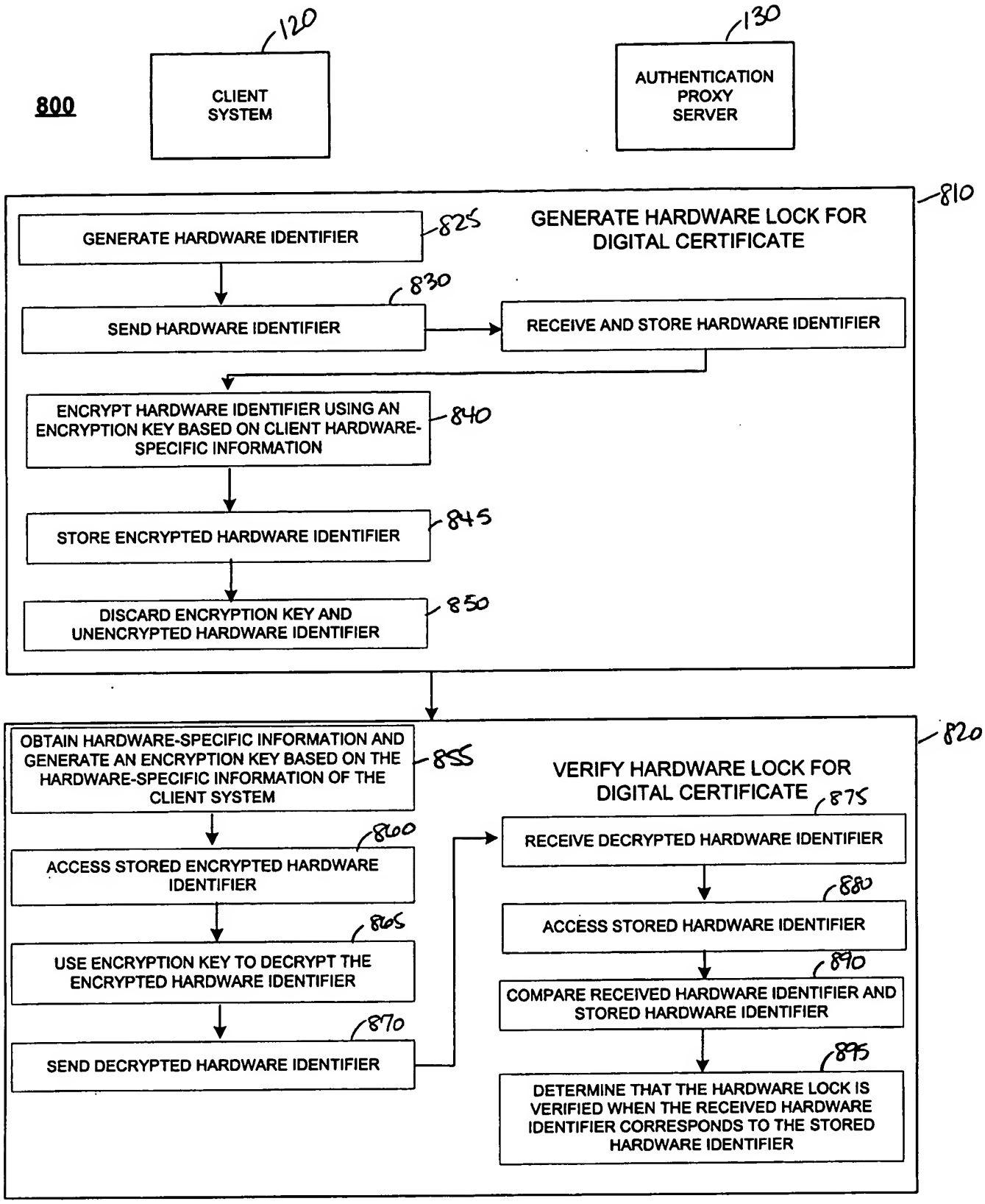
800
120
CLIENT SYSTEM
130
AUTHENTICATION PROXY SERVER
810
GENERATE HARDWARE LOCK FOR DIGITAL CERTIFICATE
825
GENERATE HARDWARE IDENTIFIER
830
SEND HARDWARE IDENTIFIER
RECEIVE AND STORE HARDWARE IDENTIFIER
840
ENCRYPT HARDWARE IDENTIFIER USING AN ENCRYPTION KEY BASED ON CLIENT HARDWARE-SPECIFIC INFORMATION
845
STORE ENCRYPTED HARDWARE IDENTIFIER
850
DISCARD ENCRYPTION KEY AND UNENCRYPTED HARDWARE IDENTIFIER
820
855
OBTAIN HARDWARE-SPECIFIC INFORMATION AND GENERATE AN ENCRYPTION KEY BASED ON THE HARDWARE-SPECIFIC INFORMATION OF THE CLIENT SYSTEM
860
ACCESS STORED ENCRYPTED HARDWARE IDENTIFIER
865
USE ENCRYPTION KEY TO DECRYPT THE ENCRYPTED HARDWARE IDENTIFIER
870
SEND DECRYPTED HARDWARE IDENTIFIER
VERIFY HARDWARE LOCK FOR DIGITAL CERTIFICATE
875
RECEIVE DECRYPTED HARDWARE IDENTIFIER
880
ACCESS STORED HARDWARE IDENTIFIER
890
COMPARE RECEIVED HARDWARE IDENTIFIER AND STORED HARDWARE IDENTIFIER
895
DETERMINE THAT THE HARDWARE LOCK IS VERIFIED WHEN THE RECEIVED HARDWARE IDENTIFIER CORRESPONDS TO THE STORED HARDWARE IDENTIFIER

FIG. 8